Cyber Threat Prioritization

FSSCC Threat and Vulnerability Assessment Committee

Jay McAllister

October 1, 2014

© 2014 Carnegie Mellon University

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Intelligence Threat Prioritization	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Jay McAllister	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**15**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-0001690

Agenda

Background: Cyber Intelligence Tradecraft Project

Cyber Threat Prioritization

Future Development: Cyber Intelligence Research Consortium

© 2014 Carnegie Mellon University

Background:
Cyber Intelligence Tradecraft Project

© 2014 Carnegie Mellon University

Cyber Intelligence Tradecraft Project

Sponsor

- National Intelligence Manager for Cyber, Office of the Director of National Intelligence (ODNI)

Purpose

- Study how organizations from industry, government, and academia perform cyber intelligence (methodologies, processes, tools, and training)

Definition of cyber intelligence

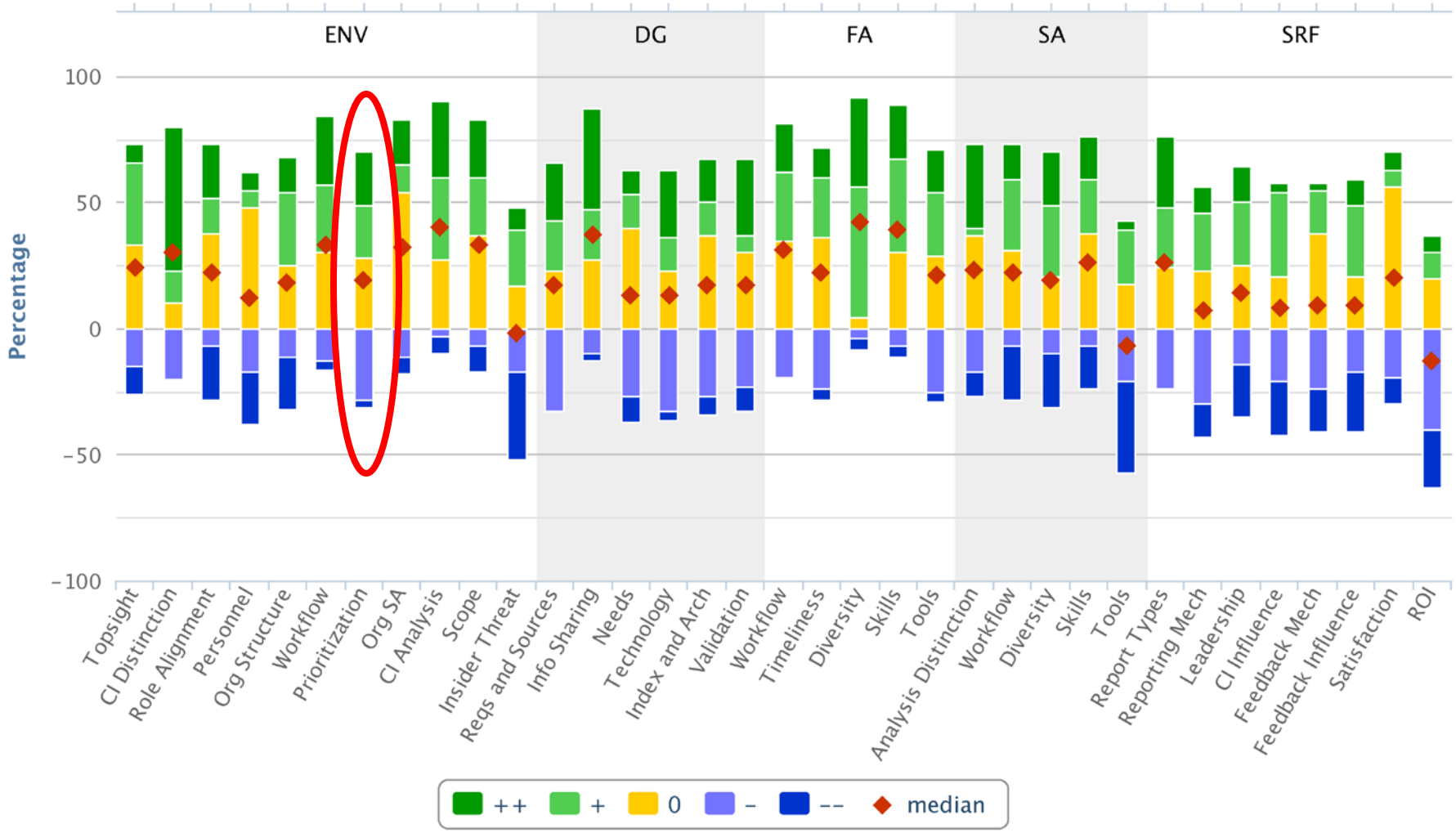
- The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making

Overall finding

- The most effective organizations balanced the need to protect their network perimeters with the need to look beyond them for strategic insights

© 2014 Carnegie Mellon University

Cyber threat baseline



© 2014 Carnegie Mellon University

Cyber Threat Prioritization

© 2014 Carnegie Mellon University

Q: How do you rank threats, from high to low?

"We consider everything a high priority threat."

- US government participant

© 2014 Carnegie Mellon University

Likelihood

Capability
An actor's sophistication, tools, and resources to execute a cyber attack determine their capability. Assessing capability as an independent variable of likelihood means organizations can avoid the pitfalls of devoting time and attention to "paper tiger" threats.

Attack Methods
Humans are creatures of habit. Although threat actors take great care to avoid detection, at some level they too succumb to this adage. Tracking how threat actors operate exposes patterns that analysts can use to combat their effectiveness.

- Infrastructure
- Technology
- Coding
- Maturity
- Targets

Resources
Understanding what is available to threat actors offers context to the sophistication of their attacks. Leverage government, industry, and intelligence service provider information sharing arrangements to learn about actors resources.

- Money
- People
- Tools
- Training

Intent
The actor's purpose and the expected outcome of the cyber attack determine the intent. Prioritizing actors by their intent allows analysts to focus on the most relevant threats.

Motive
Why do threat actors attack? Determining an actor's motive provides insight into the possible direction of their behavior, and determines their interest in targeting the organization.

- Intrinsic (personally rewarding)
- Extrinsic (receive external reward or avoid punishment)

Targeted Data
Understanding what a threat actor is after will factor into determining their intent to target the organization.

- Personally Identifiable Information (PII)
- Research and Development
- Business Process
- Industrial Control Systems

© 2014 Carnegie Mellon University

Impact

Operations

Cyber attacks adversely affect an organization's day-to-day operations. Since the effects often are financially quantifiable, analysts can use dollar amounts to communicate the impact attacks have on how an organization functions.

Direct Costs

Cyber attacks have a financial impact on organizations. Prioritizing threats according to their cost in terms of remediation and mitigation can resonate with technical and non-technical stakeholders.

- Incident Response
- Downtime
- Mitigation and/or Prevention

Business Operations

In addition to the known costs of responding to an attack, organizations also should consider the cascading effects an attack can cause and their associated costs.

- Supply Chain
- Logistics
- Future Earnings

Strategic Interests

Some impacts are harder to quantify, but they are no less important. Strategic interests capture the intangible aspects of the organization that can be affected by a cyber threat.

Organizational Interests

Plans, people, and products offer tremendous insight into why an organization is targeted and where a threat can do the most damage if certain information is compromised.

- Strategic Planning
- Stakeholders
- Organizational Culture

External Interests

Organizations do not operate in a bubble, and neither should threat prioritization. Consider the ramifications cyber attacks can have on organizational partnerships, reputation, culture, geopolitics, and market space.

- Market/Industry
- Geopolitical
- Partnerships
- Brand Reputation

© 2014 Carnegie Mellon University

Risk

People

Cyber threats generally have one thing in common; at some point a human interacts with the threat. This interaction must be a part of threat prioritization to understand an attacker's most commonly targeted vulnerability: people.

Relevance

From leadership to rank-and-file employees, the Internet offers a communication platform that allows anyone to make their organization more visible to threat actors.

- Online Presence
- Extracurricular Activities
- Motive

Access

Employees with administrator privileges or access to sensitive data are more attractive targets for threat actors. Determining who has what access can significantly aid in identifying the risk to employees.

- Physical and Network-Based Access
- Position
- Abnormal Activity

Cyber Footprint

The greater an organization's online exposure, the more opportunity an attacker has to find vulnerabilities. Consider the organization's infrastructure, supply chain, online exposure, and components most susceptible to attacks.

Infrastructure

The unknown provenance of software and hardware complicates risk determination in the cyber environment. Overcoming this limitation requires researching where, when, and how an organization's infra-structure is most susceptible to cyber threats.

- Hardware
- Software
- Supply Chain

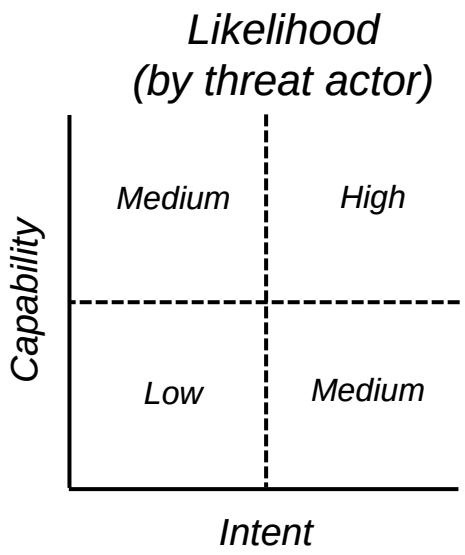
Online Presence

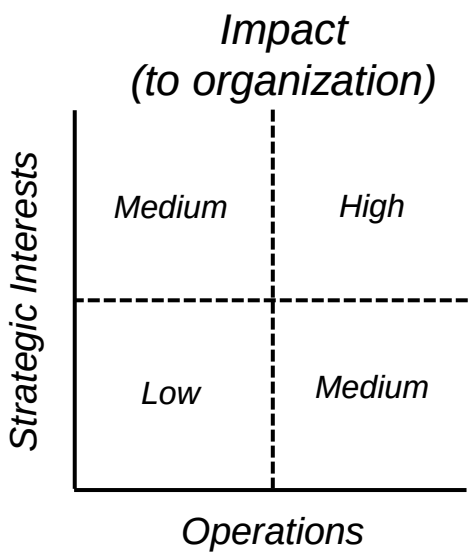
The content and services an organization provides on the Internet serve as attractive targets for threat actors. Analysts can assess severity of risk based on this insight into likely attack vectors.

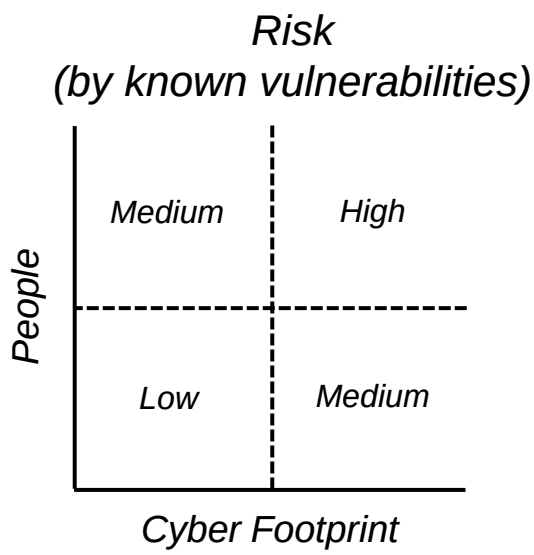
- Website
- Additional Exposure
- Additional Services

© 2014 Carnegie Mellon University

Implementing…
Threat = Likelihood + Impact + Risk







© 2014 Carnegie Mellon University

Future Development:
Cyber Intelligence Research Consortium

© 2014 Carnegie Mellon University

Cyber Intelligence Research Consortium

Purpose

- Research and develop technical solutions and analytical practices to help people make better judgments and quicker decisions with cyber intelligence

Membership

- Decision makers and practitioners from academia, Department of Defense, defense contracting, energy, financial services, and the U.S. Intelligence Community

Offerings

- Cyber threat baseline: Threat environment research to identify best practices
- Tradecraft labs: Workshops to advance analytical & technological capabilities
- Implementation frameworks: How-to guides for key intelligence practices
- Crisis simulation: Capture-the-flag exercise to apply techniques & technologies
- Intelligence insights: Continuous communication on relevant topics

© 2014 Carnegie Mellon University

Questions?

Jay McAllister
Senior Analyst – Emerging Technology Center
Software Engineering Institute – Carnegie Mellon University
412.268.9193
jjmcallister@sei.cmu.edu
@sei_etc

Tradecraft Project: http://www.sei.cmu.edu/about/organization/etc/citp.cfm

Threat Prioritization: http://www.sei.cmu.edu/about/organization/etc/citp-cyber-threat-prioritization.cfm

Consortium: http://www.sei.cmu.edu/about/organization/etc/overview.cfm

© 2014 Carnegie Mellon University